APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,981	07/16/2003	Roy M. Brooks	CIS03-25(7365)	8822

58406   7590   10/30/2007
BARRY W. CHAPIN, ESQ.
CHAPIN INTELLECTUAL PROPERTY LAW, LLC
WESTBOROUGH OFFICE PARK
1700 WEST PARK DRIVE
WESTBOROUGH, MA 01581

EXAMINER
TO, BAOTRAN N

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
10/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08/20/2007(RCE)_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-5,7-13,16-23,25 and 27-39_ is/are pending in the application.

    4a) Of the above claim(s) _6,14-15, 24 and 26 (Canceled)_ ~~is/are withdrawn from consideration~~.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-5,7-13,16-23,25 and 27-39_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____ .

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/20/2007 has been entered.

This Office action is responsive to the Applicant's Amendment filed 07/19/2007.

Claims 1, 19, and 36-39 are amended.

Claims 6, 14-15, 24, and 26 are canceled.

Claims 1-5, 7-13, 16-23, 25, and 27-39 remain for examination.

Response to Arguments

2.   Applicant's arguments filed 07/19/2007 have been fully considered but they are not persuasive.

Applicant argues, "Amended claim 1, however, was amended with dependent Claim 14, and thus the scope of amended claim 1 is exactly the same as originally filed claim 14, to recite propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism" (Page 1 of Remarks).

Examiner disagrees with this contention. This is incorrect. The dependent Claim 14 does not contain the limitation above. Applicant proposed to amend the independent Claim 1 with limitation "propagating routing information according to a predetermined protocol, the routing information operable to designate the target node as the destination of the message according to the second transport mechanism." The amended limitation changes the scope of the independent Claim 1. Therefore, it is needed for reconsideration and search.

Applicant argues, "With respect to the new rejections at hand, Ylonen '379 does not show a reroute message for rerouting in an overlay manner, as discussed further at page 5, lines 5-13. Rather, Ylonen '379 takes one of two distinct paths based on routing considerations (paragraph [0039] and source A and source B in the cited example), not on overlay path between the same endpoints" (Page 1 of Remarks).

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., rerouting in an overlay manner) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

For at least the above reasons, it is believed that the rejection is maintained.

Claim Objections

3.   Claim 1 is objected to because of the following informalities: "the filtering

complex" in line 10 should be -- **the filter complex**--. Appropriate correction is

required.

Claim 8 is objected to because of the following informalities: "The method of

claim 6" in line 1 should be ---The method of claim **1** ---- Since Claim 6 is canceled.

Appropriate correction is required.

Claims 37 is objected to because of the following informalities: "the filtering

complex" in line 21 should be -- **the filter complex**--. Appropriate correction is

required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1-5, 7-12, 16-23, 25, 27-30, 32-37 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Afek et al. (US PG Pub. 2002/0083175 A1) hereinafter Afek in

view of Ylonen et al. (US PG Pub. 2003/0110379 A1) hereinafter Ylonen.

Regarding Claim 1, Afek discloses a method for redirecting network message

traffic comprising

receiving an indication (see page 13, ¶ [0284]) of undesirable message traffic

(see page 10, ¶ [0252], "overload traffic") directed to a particular target node (page 10, ¶

[0252], victim machines) via a first transport mechanism (see page 10, ¶ [0252],

communication channel) in a communications network (see page 10, ¶ [0245]);

rerouting all message traffic (see page 13, ¶ [0286], rerouting) carried via the first

transport mechanism (see page 10, ¶ [0252], communication channel) in the

communications network (see page 10, ¶ [0245]), and directed to the particular target

node (page 10, ¶ [0252], victim machines), to a filter complex (see page 9, ¶ [0242])

operable to distinguish desirable message traffic (see page 11, ¶ [0261], appropriate

message) from undesirable message traffic (see page 10, ¶ [0252], "overload traffic");

rerouting all message traffic (see page 13, ¶ [0286], rerouting) includes directing

the filter complex from a network management server in communication with the filter

complex (see page 14, ¶ [0298]), the network management server operable to send a

reroute message to the filtering complex (see page 14, ¶ [0298]); and

directing the filtering complex (see page 9, ¶ [0242]) to transmit, via a second

transport mechanism (see page 10, ¶ [0252], secure channel as SSH) over the

communications network (see page 10, ¶ [0245]), the desirable message traffic (see

page 11, ¶ [0261], appropriate message) to the target node (page 11, ¶ [0261], victim

machines),

directing the filter complex further comprises propagating routing information

according to a predetermined protocol (see page 2, ¶ [0016]).

Afek does not disclose "routing information operable to designate the target

node, as the destination of the message according to the second transport mechanism."

However, Ylonen expressly discloses routing information operable to designate

the target node, as the destination of the message according to the second transport

mechanism (see page 3, ¶ [0039]).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to have incorporated Ylonen's reference with Afek to

include routing information operable to designate the target node, as the destination of

the message according to the second transport mechanism. One of ordinary skill in the

art would have been motivated to do so because the processed packet should be

directed towards their original destination as taught by Ylonen (see page 3, ¶ [0026]).

Regarding Claims 19 and 37, Afek discloses a network management server (see

page 10, ¶ [0252], "NOC (Network Operations Center)", "SNMP") for redirecting

undesirable message traffic (see page 10, ¶ [0252], "overload traffic") comprising:

a network intrusion detector monitor operable to receive an indication (see page

10, ¶ [0252], sending authenticated messages, signal) of undesirable message traffic

(see page 10, ¶ [0252], "overload traffic") directed to a particular target node (page 10, ¶

[0252], victim machines) via a first transport mechanism in a communications network

(see page 10, ¶ [0252], communication channel);

a routing processor operable to propagate routing information from a routing

table database to reroute all message traffic (see page 10, ¶ [0252], diverting routers)

using the first transport mechanism (see page 10, ¶ [0252], communication

channel).directed to the particular target node (page 10, ¶ [0252], victim machines); and

a connection to a filter complex responsive to the rerouting processor (see page

10, ¶ [0252], the guards), the filter complex operable to distinguish desirable message

traffic from undesirable message traffic (see page 13, ¶ [0288]), and further operable to

transmit, via a second transport mechanism (see page 10, ¶ [0252], secure channel as

SSH) over the communications network, the desirable message traffic (see page 11, ¶

[0261], appropriate message) to the target node (page 11, ¶ [0261], victim machines),

rerouting all message traffic (see page 13, ¶ [0286], rerouting) further comprises

propagating, via a standard protocol (see page 9, ¶ [0241], Internet) corresponding to

the first transport mechanism, a node address other than the node address

corresponding to the target node (page 11, ¶ [0261], victim machines),

the routing processor operable to direct the filter complex to propagate routing

information according to a predetermined protocol (see page 2, ¶ [0016]),

Afek does not disclose "routing information operable to designate the target

node, as the destination of the message according to the second transport mechanism."

However, Ylonen expressly discloses routing information operable to designate

the target node, as the destination of the message according to the second transport

mechanism (see page 3, ¶ [0039]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Ylonen's reference with Afek to include routing information operable to designate the target node, as the destination of the message according to the second transport mechanism. One of ordinary skill in the art would have been motivated to do so because the processed packet should be directed towards their original destination as taught by Ylonen (see page 3, ¶ [0026]).

Afek and Ylonen disclose the limitations of Claim 19 above. Afek further discloses the network management server further operable to send a reroute message to the filtering complex (see page 14, ¶ [0298]), in response to which the filter complex is operable to reroute the message traffic, the reroute message (see page 10, ¶ [0252]) indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node (see page 8, ¶ [0214]) via the target node router serving the target node (see page 2, ¶ [0016], victim).

Regarding Claim 36, Afek discloses in a network management server (see page 10, ¶ [0252], "NOC (Network Operations Center)", "SNMP") of a networked system of data communications devices, a method for transparently intercepting, filtering, and rerouting message traffic for recovering from a distributed denial of service attack comprising:

detecting (see page 2, ¶ [0019]; page 13, ¶ [0282]), at a network monitor in the network management server, a pattern of inundating undesirable message traffic (see page 10, ¶ [0252], "overload traffic") to a particular target node (page 10, ¶ [0252],

victim machines) via a first transport mechanism (see page 10, ¶ [0252], communication channel) in a communications network (see page 10, ¶ [0245]);

receiving, via a routing processor, an indication (see page 13, ¶ [0284]) of the undesirable message traffic (see page 10, ¶ [0252], "overload traffic") directed to the particular target node (page 10, ¶ [0252], victim machines);

transmitting, via a network interface, a reroute message (see page 1, ¶ [0011], page 13, ¶ [0284]) to a filter complex (see page 13, ¶ [0284], guard machines) having a security filter operable to distinguish desirable message traffic (see page 11, ¶ [0261], appropriate message) from undesirable message traffic (see page 10, ¶ [0252], "overload traffic"); and

rerouting, via a filter routing device in the filter complex, all message traffic (see page 13, ¶ [0286]) carried via the first transport mechanism (see page 10, ¶ [0252], communication channel) in the communications network (see page 10, ¶ [0245]) and directed to the particular target node (see page 10, ¶ [0252], victim machines);

rerouting all message traffic (see page 13, ¶ [0286], rerouting) includes directing the filter complex from a network management server in communication with the filter complex (see page 14, ¶ [0298]), the network management server operable to send a reroute message to the filtering complex (see page 14, ¶ [0298]), the reroute message (see page 10, ¶ [0252]) indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node (see page 8, ¶ [0214]) via the target node router serving the target node (see page 2, ¶ [0016], victim);

filtering, at the security filter, the message traffic to bifurcate (see page 13, ¶ [0293]) desirable message traffic (see page 11, ¶ [0261], appropriate message) from undesirable message traffic (see page 10, ¶ [0252], "overload traffic"); transmitting, via the network interface to a target node router serving the target node, a redirect message indicating that the target node router is to receive (see page 1, ¶ [0011]), via the second transport mechanism (see page 10, ¶ [0252], secure channel as SSH), the desirable message traffic (see page 11, ¶ [0261], appropriate message) directed to the particular target node and rerouted to the filter complex (see page 13, ¶ [0293]), the filter complex and the target node router conversant in the first transport mechanism (see page 10, ¶ [0252], communication channel)and the second transport mechanism (see page 10, ¶ [0252], secure channel as SSH); and

directing, from the network management server, the filtering complex to transmit, via a second transport mechanism (see page 10, ¶ [0252], secure channel as SSH) over the communications network (see page 10, ¶ [0245]), the desirable message traffic to the target node (see page 11, ¶ [0261]),

directing the filter complex further comprises propagating routing information according to a predetermined protocol (see page 2, ¶ [0016]).

Afek does not disclose "routing information operable to designate the target node, as the destination of the message according to the second transport mechanism."

However, Ylonen expressly discloses routing information operable to designate the target node, as the destination of the message according to the second transport mechanism (see page 3, ¶ [0039]).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to have incorporated Ylonen's reference with Afek to

include routing information operable to designate the target node, as the destination of

the message according to the second transport mechanism. One of ordinary skill in the

art would have been motivated to do so because the processed packet should be

directed towards their original destination as taught by Ylonen (see page 3, ¶ [0026]).

Regarding Claims 2 and 20, Afek and Ylonen disclose directing the filter complex

to filter the message traffic (see page 10, ¶ [0253]) to subdivide desirable message

traffic (see page 11, ¶ [0261], appropriate message) from undesirable message traffic

(see page 10, ¶ [0252], "overload traffic"; page 13, ¶[0288]).

Regarding Claims 3 and 21, Afek and Ylonen disclose wherein the filter complex

further comprises a security filter having filtering logic for performing filtering (see page

13, ¶ [0293], rules), the security filter operable to parse the message traffic and identify

sequences in the message traffic indicative of undesirable message traffic (see page

13, ¶ [0288] & [0295]).

Regarding Claims 4 and 22, Afek and Ylonen disclose wherein the filter complex

further includes a filter routing device in communication with other routing devices in the

communications network (see page 14, ¶ [0301], "working in connection with the

routers") and coupled to the security filter for analyzing message traffic (see page 13, ¶

[0293] & ¶ [0295]).

Regarding Claims 5 and 23, Afek and Ylonen disclose wherein the filter routing

device (see page 14, ¶ [0304]) in the filtering complex (see page 14, ¶ [0291], element

10) is operable to communicate according to the first transport mechanism (see page

10, ¶ [0252], communication channel) and the second transport mechanism (see page

10, ¶ [0252], secure channel as SSH).

Regarding Claims 7 and 25, Afek and Ylonen disclose directing a target node

router serving the target node (page 11, ¶ [0261], victim machines) from the network

management server (see page 10, ¶ [0252]), the network management server operable

to send a redirect message to the target node router (see page 1, ¶ [0015]; page 14, ¶

[0298]).

Regarding Claim 8, Afek and Ylonen disclose the reroute message (see page 10,

¶ [0252]) is indicative of the filtering complex receiving message traffic according to the

first transport mechanism intended for the target node (see page 8, ¶ [0214]) via the

target node router serving the target node (see page 2, ¶ [0016], victim).

Regarding Claims 9 and 27, Afek and Ylonen disclose wherein the redirect

message (see page 11, ¶ [0257], alert) is indicative that the target router serving the

target node is not to receive message traffic (see page 11, ¶ [0257]) according to the

first transport mechanism corresponding to the target node (see page 11, ¶ [0257],

victim).

Regarding Claims 10 and 28, Afek and Ylonen disclose wherein the redirect

message is indicative that the target node router (see page 13, ¶ [0290]) serving the

target node (see page 10, ¶ [0247], "potential victims") receives the desirable message

traffic in the second transport mechanism corresponding to the target node.

Regarding Claims 11 and 29, Afek and Ylonen disclose wherein first and second

transport mechanisms coexist on a common physical network (see Figure 1, page 9, ¶

[0240]).

Regarding Claims 12 and 30, Afek and Ylonen disclose wherein first transport

mechanism corresponds to a public access protocol (see page 9, ¶ [0241], IP network)

adapted for communication via a plurality of dissimilar network switching devices (see

page 9, ¶ [0241], "switches").

Regarding Claim 32, Afek and Ylonen disclose wherein rerouting all message

traffic (see Afek page 13, ¶ [0286], rerouting) further comprises propagating, via a

standard protocol (see Afek page 9, ¶ [0241], Internet) corresponding to the first

transport mechanism, a node address other than the node address corresponding to the target node (page 11, ¶ [0261], victim machines).

Regarding Claim 33, Afek and Ylonen disclose wherein directing the filter complex further comprises propagating routing information according to a predetermined protocol (see Afek page 2, ¶ [0016]), the routing information operable to designate the target node (see Afek page 2, ¶ [0016], victim) as the destination of the message according to the second transport mechanism (see Ylonen page 3, ¶ [0026]).

Regarding Claims 16 and 34, Afek and Ylonen disclose wherein rerouting all message traffic is a static route (see page 2, ¶ [0016]; page 11, ¶ [0267]), according to the first transport mechanism (see page 10, ¶ [0252], communication channel), from a single router serving the target node (see abstract, "second set") to the filter router (see page 14, ¶ [0304]) serving the filter complex (see fig. 2).

Regarding Claim 17, Afek and Ylonen disclose wherein receiving an indication (see page 13, ¶ [0284]) further comprises detecting a recognizable pattern of inundating undesirable message traffic (see page 3, ¶ [0039]).

Regarding Claims 18 and 35, Afek and Ylonen disclose wherein the undesirable message traffic (see page 10, ¶ [0252], "overload traffic") emanates from a plurality of sources (see page 1, ¶ [0002], DDOS), each of the plurality of sources independently

contributing substantially insignificant volume of message traffic (see page 1, ¶ [0002],

DDOS).

5.   Claims 13 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Afek and Ylonen applied to claims 1 and 19 above, and further in view of Desai et

al (U.S. PG Pub 2003/0188189) hereinafter Desai.

        Regarding Claims 13 and 31, Afek and Ylonen disclose all the limitations above.

Afek and Ylonen do not disclose wherein the second transport mechanism corresponds

to a virtual private network operable to encapsulate message packets of dissimilar

protocols such that the encapsulated message packets are recognized by a routing

protocol of the virtual private network.

        However, Desai expressly discloses wherein the second transport mechanism

corresponds to a virtual private network" (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs)

operable to encapsulate message packets of dissimilar protocols such that the

encapsulated message packets are recognized by a routing protocol of the virtual

private network (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs).

        Therefore, it would have been obvious at the time the invention was made to a

person having ordinary skill in the art to which said subject matter pertains to have

modified Ylonen's reference with Afek which disclose use of SSH (see Afek, page 10, ¶

[0252], "SSH") to include the use of Virtual private network like in Desai's reference for

the purpose to ensure secure data transfer (see Desai, page 3, ¶ [0044]).

6.   Claim 38 is rejected under 35 U.S.C. 103(a) as being unpatentable over Afek et

al. (US PG Pub. 2002/0083175 A1) hereinafter Afek in view of Ylonen et al. (US PG

Pub. 2003/0110379 A1) hereinafter Ylonen and further in view of Desai et al (U.S. PG

Pub 2003/0188189) hereinafter Desai.

Regarding Claim 38, Afek discloses an encoded set of processor based

instructions tangible encoded on a computer readable medium embodying program

code for redirecting network message traffic comprising:

program code for receiving an indication (see page 13, ¶ [0284]) of undesirable

message traffic (see page 10, ¶ [0252], "overload traffic") directed to a particular target

node (page 10, ¶ [0252], victim machines) via a first transport mechanism (see page 10,

¶ [0252], communication channel) in a communications network (see page 10, ¶

[0245]);

program code for rerouting all message traffic (see page 13, ¶ [0286], rerouting)

carried via the first transport mechanism (see page 10, ¶ [0252], communication

channel) in the communications network (see page 10, ¶ [0245]), and directed to the

particular target node (page 10, ¶ [0252], victim machines), to a filter complex (see page

9, ¶ [0242]) operable to distinguish desirable message traffic (see page 11, ¶ [0261],

appropriate message) from undesirable message traffic (see page 10, ¶ [0252],

"overload traffic"); rerouting all message traffic (see page 13, ¶ [0286], rerouting)

includes directing the filter complex from a network management server in

communication with the filter complex (see page 14, ¶ [0298]), the network

management server operable to send a reroute message to the filtering complex (see

page 14, ¶ [0298]), the reroute message (see page 10, ¶ [0252]) indicative of the

filtering complex receiving message traffic according to the first transport mechanism

intended for the target node (see page 8, ¶ [0214]) via the target node router serving the

target node (see page 2, ¶ [0016], victim);

means for filter complex further comprises: means for propagating routing

information according to a predetermined protocol (see page 2, ¶ [0016]).

Afek does not disclose "routing information operable to designate the target

node, as the destination of the message according to the second transport mechanism."

However, Ylonen expressly discloses routing information operable to designate

the target node, as the destination of the message according to the second transport

mechanism (see page 3, ¶ [0039]).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to have incorporated Ylonen's reference with Afek to

include routing information operable to designate the target node, as the destination of

the message according to the second transport mechanism. One of ordinary skill in the

art would have been motivated to do so because the processed packet should be

directed towards their original destination as taught by Ylonen (see page 3, ¶ [0026]).

Afek and Ylonen disclose all the limitations of Claim 38 above. Afek and Ylonen

do not disclose "wherein the second transport mechanism corresponds to a virtual

private network operable to encapsulate message packets of dissimilar protocols such

that the encapsulated message packets are recognized by a routing protocol of the
virtual private network."

However, Desai expressly discloses wherein the second transport mechanism
corresponds to a virtual private network" (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs)
operable to encapsulate message packets of dissimilar protocols such that the
encapsulated message packets are recognized by a routing protocol of the virtual
private network (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs).

Therefore, it would have been obvious at the time the invention was made to a
person having ordinary skill in the art to which said subject matter pertains to have
modified Desai's reference with Afek and Ylonen which disclose use of SSH (see Afek,
page 10, ¶ [0252], "SSH") to include the use of Virtual private network like in Desai's
reference for the purpose to ensure secure data transfer (see Desai, page 3, ¶ [0044]).

7.   Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Afek et
al. (US PG Pub. 2002/0083175 A1) hereinafter Afek in view of Desai et al (U.S. PG Pub
2003/0188189) hereinafter Desai.

Regarding Claim 39, Afek discloses a network management server for redirecting
undesirable message traffic comprising;

means for receiving an indication (see page 13, ¶ [0284]) of undesirable
message traffic (see page 10, ¶ [0252], "overload traffic") directed to a particular target
node (page 10, ¶ [0252], victim machines) via a first transport mechanism (see page 10,

¶ [0252], communication channel) in a communications network (see page 10, ¶ [0245]);

means for rerouting all message traffic (see page 13, ¶ [0286], rerouting) carried via the first transport mechanism (see page 10, ¶ [0252], communication channel) in the communications network (see page 10, ¶ [0245]), and directed to the particular target node (page 10, ¶ [0252], victim machines), to a filter complex (see page 9, ¶ [0242]) operable to distinguish desirable message traffic (see page 11, ¶ [0261], appropriate message) from undesirable message traffic (see page 10, ¶ [0252], "overload traffic"); rerouting all message traffic (see page 13, ¶ [0286], rerouting) includes directing the filter complex from a network management server in communication with the filter complex (see page 14, ¶ [0298]), the network management server operable to send a reroute message to the filtering complex (see page 14, ¶ [0298]), the reroute message (see page 10, ¶ [0252]) indicative of the filtering complex receiving message traffic according to the first transport mechanism intended for the target node (see page 8, ¶ [0214]) via the target node router serving the target node (see page 2, ¶ [0016], victim); and means for directing the filtering complex (see page 9, ¶ [0242]) to transmit, via a second transport mechanism (see page 10, ¶ [0252], secure channel as SSH) over the communications network (see page 10, ¶ [0245]), the desirable message traffic (see page 11, ¶ [0261], appropriate message) to the target node (page 11, ¶ [0261], victim machines).

Afek does not disclose wherein the second transport mechanism corresponds to a virtual private network operable to encapsulate message packets of dissimilar

protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network.

However, Desai expressly discloses wherein the second transport mechanism corresponds to a virtual private network" (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs) operable to encapsulate message packets of dissimilar protocols such that the encapsulated message packets are recognized by a routing protocol of the virtual private network (see page 1, ¶ [0012]; page 3, ¶ [0044], VPNs).

Therefore, it would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have modified Desai's reference with Afek which disclose use of SSH (see Afek, page 10, ¶ [0252], "SSH") to include the use of Virtual private network like in Desai's reference for the purpose to ensure secure data transfer (see Desai, page 3, ¶ [0044]).

Contact Information

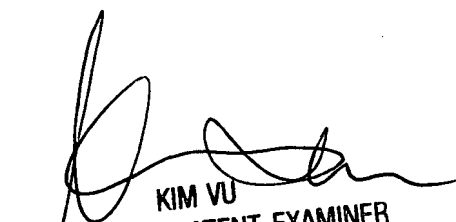8.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BT
10/22/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100